Module 11

Desktop Computer Security

11.1 OBJECTIVES

Students will be able to:

- Summarize the elements of desktop computer security in relations to information superiority
- Identify the basic application of desktop computer security safeguards
- List common types of client computer security risks
- Match audit events with the potential threat the audit events monitor
- Summarize the permissions granted to the four default groups

11.2 OVERVIEW

According to AFI 33-202 (Computer Security) "*Workgroup managers (WM) may perform some or all of the duties as listed below:*

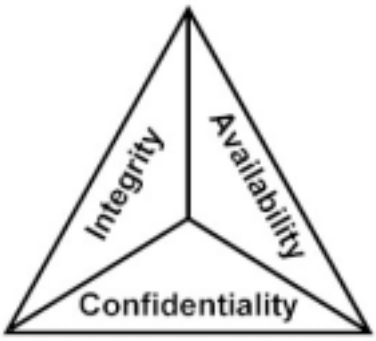
> *Establish controls to ensure users operate, maintain, and dispose of information systems according to existing policies and procedures, including the (Air Force and unit) system security policy.*
>
> *Ensure the system security policy for each information system is distributed to system users.*
>
> *Establishes controls that ensure audit trails are periodically reviewed."*

This presents workgroup managers with the task of becoming an intricate part of safeguarding computer systems and information against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or the unauthorized releasing of classified and confidential information.

Workgroup managers must also protect hardware, firmware, software, and information against unauthorized disclosure, destruction, or modification. This requirement dictates that the workgroup managers are an intricate part of the Air Force vision of Information Security, and the focal point of desktop security.

11.3 INFORMATION SUPERIORITY

Information superiority is the concept of providing desktop users with secure single point access to required/relevant information. Workgroup managers contribute to the Air Force mission of information superiority by implementing the information security triad--*confidentiality, integrity, and availability.*



Confidentiality: Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of information or data systems. Loss of confidentiality can occur in many ways. For

example, loss of confidentiality may occur by the intentional release of classified or confidential information or though a misapplication of network rights and access.

Some of the elements of telecommunication used to ensure confidentiality are:

- Network security protocols (IPSec, SSH2, SSL, protocols)
- Network authentication services (Kerberos 5 in Windows 2000)
- Data encryption services

Integrity: Making sure that the data has not been changed due to an accident or malice. Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered. Loss of integrity can occur either through an intentional attack (for example: a website defacement) or, by the most common type: an operator alters data accidentally. A critical part of desktop security is the assurance that only intended sources can access designated workstation, with no disruption of data integrity.

Some of the elements used to ensure integrity are:

- Firewalls services
- Communications Security Management techniques
- Intrusion detection services (i.e. CIDDS/ASIM)

Availability: Ensuring data is accessible when and where needed. This concept refers to the elements that create reliability and stability in networks and systems, which assures that connectivity is accessible where needed, allowing authorized users to access network or systems.

Also included is the guarantee that security services for the security are usable when they are needed. The concept of availability also includes areas in the Information Systems that are traditionally not thought of as pure security (such as guarantee of service, performance, client satisfaction and workstation up-time), yet are obviously affected by an attack like a Denial of Service (DOS).

Some of the elements that ensure availability are:

- Fault tolerance for data availability, such as backups and redundant disk systems
- Acceptable log-ins and operating process performances
- Reliable and interoperable security processes and network security mechanisms

11.4 DESKTOP COMPUTER SECURITY

Desktop computer security is the active process of securing all operational data and client access within the computing environment. Desktop computer security encompasses all personal computers, workstations functioning as stand-alone systems, terminals or client networking systems.

Desktop computer security is just one aspect of the larger network security topology. Desktop security is one of the practices utilized by

the Air Force to obtain information superiority. Computer security also includes the process of preventing and detecting intrusions into the desktop environment. Preventive measures help you keep intruders from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

Desktop security consists of both physical and logical security. In order to secure desktop communications, physical access to the desktop computers, cable or other media, and network devices must be controlled. Logical security barriers, such as user authentication methods, encryption, and so on, must also be in place. Another way to think of these two divisions is hardware security and software security.

A prime example of physical security can be found at most Major Command Network Operations Security Centers (NOSC) and Network Control Centers (NCC). These are network centers that house both desktop and server computers. At both facilities mission essential computers are maintained with a high degree of physical security to include:

- Cipher locked entries
- Badge access requirements
- "Need to know" only access requirements

An example of software security can be found in the authentication process of the Windows 2000 Professional desktop operating system. Window 2000 Professional provides software security through authentication (*The process of validating the identity of a user or a device such as a server or router. There are a number of different methods of authenticating identity, including Keberos, NTLM, RADIUS, and many others).*

Windows 2000 Authentication process

- The user supplies logon information, such as user name and password, which is passed on to the local security subsystem of the local computer.
- The security subsystem of the local computer contains the local security database that Windows 2000 uses to validate the logon information.
- If the logon information matches and the user account are valid, Windows 2000 creates an access token for the user.
- An access token is the user's identification for the local computer.
- The access token contains the user's security settings.
- The security settings allow the user to gain access to the appropriate resources and to perform specific system tasks.

11.4.1. BASICS OF SECURE DESKTOP COMPUTING

Single Sign-on. The ability of users to provide one username and password to access all authorized network resources, such as printer, files, applications, and various network functions, rather than having to be authenticated separately for multiple servers and applications. The single sign-on function enables security to be managed in as a centralized component.

Access Control. The method of protecting resources by assigning or denying permissions. Both Desktop and Network Administrators utilize various access control techniques to ensure the protection of files, directory, classified printers and other secure resources.

Data Integrity. Protecting network data against tampering and modification or destruction. To include sniffers, probes, contaminations, interception, data impersonation, and denial of service attacks.

Data Confidentiality. The ability to encrypt data before it is transferred over the network so that someone eavesdropping or "tapping" the network cannot read it.

Physical Security. Protection of the network's physical assets (servers, workstations, cable, hubs, and so on) from intruders.

User Education. The best Air Force security plan in the world will fail if users are not educated to keep their passwords secret and guard against distribution of confidential information. AFI 33-115 Para 4-1, States that, *"Every individual who has access to the Air Force network (af.mil) domain, specialized systems, and mission systems is a network user. Before becoming an Air Force network user an individual must be trained and licensed."* As new threats, risk and vulnerabilities continue to arise, the workgroup manager must be prepared to train, equip, and direct users to a posture of security. It is well documented that increasing the knowledge and awareness of the end user can prevent many contaminations, virus propagations, and security vulnerabilities. This is a valuable component of the Air Force's Information Superiority mission.

Workstation Security. Users work on desktop computers, laptops, and mobile devices. While controlling access to the building or area is essential, there are risks of laptops or mobile devices being removed from the user's workspace. Perhaps more importantly, is the unrestricted access to devices connected to the network that the user's workspace provides. To protect the computers in the user's workspace, a network administrator should consider implementing the following security measures:

- **Restricted Access.** The best security is physically restricting access to work areas where workstations are present. However, this is impractical in many organizations. Therefore, ensuring that anyone accessing these areas is at least authorized to be in the building will reduce security risks. In addition, user logon rights can be further restricted. These rights can be managed with a user rights policy applied at the server or client level.

- **Client PC Hard Drives.** As mentioned earlier, securing or restricting access to the facility or the workspace is the first line of defense. The second line of defense is protecting the data on local hard drives. Data can be protected in several ways:

    1. **Require users to store data files on network servers if the option is available.** End users typically do not back up their data. Therefore, rather than leaving the data on local hard drives exposed to loss (through theft or mechanical failure), critical data files can be stored on the network. Since network data shares are routinely backed up, user data is protected.

    2. **Back Up Early and Often.** People who don't back up their information run the risk of losing that information. If the user's hard disk crashes, there may be no way to retrieve the information on the disk. Years of accumulated data could be

lost. If a virus destroys system or data files or if the system is stolen…there goes all the data.

Microsoft and a variety of other companies provide software tools that enable users to back up information and data files removable medium (floppy disk, Zip disk, tape, or CD). As long as users have a current backup of files, no more than a day or two of work will be lost.

Use the NTFS file system. Users' local hard drives can be formatted using FAT or New Technology File System (NTFS), depending on which Windows operating system they are running. Installing Windows NT or Windows 2000 enables the formatting of partitions and disks using the NTFS file system format. The NTFS file system allows users to control access to files, even if an unauthorized user gains access to the local machine. By restricting access to files and folders, users can ensure that data is secure against unauthorized access.

11.4.2 ACCESS CONTROL

Strong Passwords. Strong password policy is vital to end-user and network security. Enforcing the sophisticated password policies dramatically reduces the chance of hackers gaining access through password breaches.

The enforcement of password can be done at the network or client level depending on network policy. Examples of strong password and password policies that can be set at the desktop or client level are below:

- Set the minimum password length to at least 8 characters
- Set a minimum password age appropriate to your network (typically between 1 and 7 days)
- Set a maximum password age appropriate to your network (typically no more than 42 days)
- Set a password history maintenance (using the "Remember passwords" option) of at least 6

Elements of a Strong Password Policy.

Password element	Benefit and Risk
Length greater than eight characters.	The number of possible combination of characters is 8^7, or 2,097,152 combinations. This significantly reduces the chances of a lucky guess.
Require upper and lower case, numbers, and symbols.	This prevents simple dictionary cracking programs from working. Dictionary cracking programs run words from a dictionary through the system in an attempt to discover passwords.
Password uniqueness (cannot use password similar to previous ones).	Users often choose Monday1, and when forced to change their password will choose Monday2—it's easy to remember. However, it makes it easy to crack a password. Requiring uniqueness so that the new password cannot contain too many similarities to the expired password is recommended.
Password cannot contain user ID.	Related to requiring a unique password, passwords should not contain the user's first or last name or any part of the user's network username.
Passwords cannot repeat.	Users also tend to want to reuse passwords. Setting the system to save previous passwords prevents repeated patterns.
Password must change at first logon.	When a new user account is set up, the administrator can (and should) require the password to be reset immediately.

Password-protected screen savers. By requiring the use of password-protected screen savers, unauthorized users cannot gain access to the system without rebooting. Rebooting the system requires authentication to access network resources. If the system is using NTFS and EFS, unauthorized users will be limited to physically removing the device from the premises in order to gain access to the data.

Lock the Workstation. In Windows NT 4.0 and 2000, pressing Ctrl+Alt+Del and clicking Lock Computer, you can prevent unauthorized individuals from gaining access to the computer. Only the user and members of the Administrators group on that system can unlock it. You can also set up a screen saver so that whenever the computer is idle for more than a specified length of time, the screen saver starts and the computer automatically locks. To unlock the computer, press Ctrl+Alt+Del, type your

password, then click Ok. Also, if computers are shared by users (for instance, those working on different shifts), ensure that users sign off their computers at the end of their shift.

Disable unnecessary services.

After installing Windows NT 4.0 or 2000, disable any network services not required for the computer. In particular, consider whether the client system needs any Internet Information Service Web services and disable them under the administrator account.

Disable or delete unnecessary accounts.

Review the list of active accounts (for both users and applications) on the system and disable any non-active accounts and delete accounts, which are no longer required.

Protect files and directories.

Refer to Default Access Control Settings for on the Microsoft TechNet Security Web site for details on the default file system Access Control Levels and how to make any necessary modifications.

Disable guest accounts.

By default, the Guest account is disabled on systems running Windows NT 4.0 or 2000. If the Guest account is enabled, disable it.

Install antivirus software and updates.

It is imperative to install antivirus software and keep up-to-date on the latest virus signatures on all Internet and intranet systems. Most systems on base-wide networks apply a script that will automatically update virus software and updates at the time of sign-on. WMs need to periodically review all systems to ensure virus updates are being applied. More security antivirus information is available on the Microsoft TechNet Security Web site at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/virus.asp.

Install Service Packs.

Each Service Pack for Windows includes all security fixes from previous Service Packs. Keep up-to-date on Service Pack releases and install Service Packs as determined by the Base NCC. The current Service Pack for Windows 2000, SP2, is available at: Windows 2000 Service Pack 2. Service Packs are also available through Microsoft Product Support. Information about contacting Microsoft Product Support is available at http://support.microsoft.com/support/contact/default.asp.

Post-Service Pack security hot fixes.

The Air Force Network Operations Center (AFNOC) will, from time-to time, issue security bulletins on Microsoft and other products. These bulletins will direct a wide range of changes, from network security posture to updates on software. Do not apply security changes based solely on recommendations from software manufactures. Only take direction from the NCC, NOSC or AFNOC. If there are concerns bring them to the NCCs attention for review.

11.5 DETERMINING TYPES OF SECURITY RISKS

In analyzing the desktop security requirements of Air Force organizations, WMs must understand what types of security risks to protect against, and establish priorities. Common types of security risks and network attacks in the Air Force environment include:

Identity interception. Unauthorized access is gained by using the valid credentials of someone else.

Impersonation. The ability of an unauthorized person to present credentials that appears to be valid (see replay attack).

Replay attack. An unauthorized user records the exchange of packets between an authorized user and the server, and plays it back later.

Masquerading. An unauthorized user uses the IP address of a trusted system account or device.

Data interception. Consists of monitoring and capturing data as it is transferred across the network.

Manipulation. Unauthorized modification of unencrypted data.

Repudiation. The identity of the sender cannot be verified.

Denial of service attacks. Server is flooded with numerous requests that use all the bandwidth or resources so that the server cannot communicate.

Trojan horse. A virus or malicious program that is disguised as a harmless program.

Social engineering. This is the term used for breaking into a network by simply "outwitting" employees and convincing them to reveal their passwords. Often the intruder pretends to be with the organizations IT department and tells the users that he is verifying their password or that there is a problem with their network account.

Malicious code. This is a method of attacking a network by embedding ActiveX, VB script, or a Java applet in a web page or e-mail message, which when executed will provide the intruder with a way to access information on the network which he or she is not authorized to access.

Macro viruses. Macros are small programs that run inside other programs; for example, macros can be written to automate commonly used functions in Microsoft Word and other word processing programs. A macro virus uses this capability to invade a system and cause damage or gain unauthorized access to data.

11.5.1 AUDITING

Auditing allows network personnel to monitor the use (and misuse) of the network and take appropriate action as needed. Auditing creates log files on the client system that workgroup managers should review

periodically to ensure that network access has not been compromised. The following table lists audit events you can log, and the specific threat these audit events monitor:

Audit Event	Potential Threat
Failure audit for logon/logoff	Random password hack
Success audit for logon/logoff	Stolen password break-in
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events	Misuse of privileges
Success and failure audit for file-access printers and object-access events	Improper access to printers
Success and failure write access auditing for programs (.EXE and .DLL extensions)	Virus outbreak

Setting network servers and clients to audit too many events will degrade performance. Large audit files must be reviewed, and identifying relevant data will become quite difficult. Choosing to audit the failure of events often provides more meaningful information. Choose audit events that meet the needs of the organization.

11.5.2 REMOTE AND MOBILE USERS

Data protection for remote users is more difficult simply because the users are outside the secure computing environment. In this section, we will discuss the two remote user groups: mobile users and remote site users. In all cases, user account options provide the network administrator with a number of advanced security options. Assigning users to the proper groups, assigning permissions to groups appropriately, and enforcing logon requirements (logon hours, password requirements, etc.) are the most basic steps to securing any user account, be it local or remote. We will cover the similarities and differences in protecting data for mobile users versus remote site users. We will also discuss various data transmission risks for both mobile and remote users, and we will look at the tools that Windows 2000 provides to secure data transmission.

There are three risks for mobile users: loss of equipment, loss of data through equipment failure (hard disk crash), and interception of data being transmitted. We will discuss each of these risks and the associated methods of mitigating each risk in this segment.

Protecting mobile user equipment from loss is difficult. Laptops, Palmtops, Pocket PCs, or other Personal Digital Assistants (PDAs) can easily be picked up and carried off at airports, car rental counters, and unfortunately, even at the user's desk. Keeping track of equipment serial numbers and providing locking devices on desks are about the only feasible methods of protection against actual loss of equipment.

Physical data protection for mobile users is a difficult task. It is important to encourage users to make regular backups of their data when they are connected to a local backup device or the corporate network will protect them in the event of disk failure. Creating home directories for users can encourage users to

store critical files on network servers rather than on local hard drives. This has both positive and negative consequences. The upside is that corporate servers are backed up regularly; therefore, data loss should be minimal.

The downside is that a user may not have data available on their hard drive when needed. Connecting to the corporate network to get a critical data file may be time consuming or overly burdensome for the mobile user. Encouraging users to store files locally and back them up to servers when connected to the network is a good intermediate solution.

If the mobile device is stolen, using the NTFS file system and the EFS encryption system (Windows 2000 only) will protect the data on the device. File encrypting will keep the data from easily being recovered. The EFS encryption system encrypts files so that only the user can decrypt them. EFS should not be used for shared files, or data on a network server. For physical data protection on a mobile device, NTFS combined with EFS is excellent protection against confidential data being compromised. Encouraging users to secure their device with password-protected screen savers, or using Ctrl+Alt+Del to lock the device when not in use, will provide another line of defense against unauthorized access to information.

11.6 WINDOWS 2000 PROFESSIONAL SECURITY

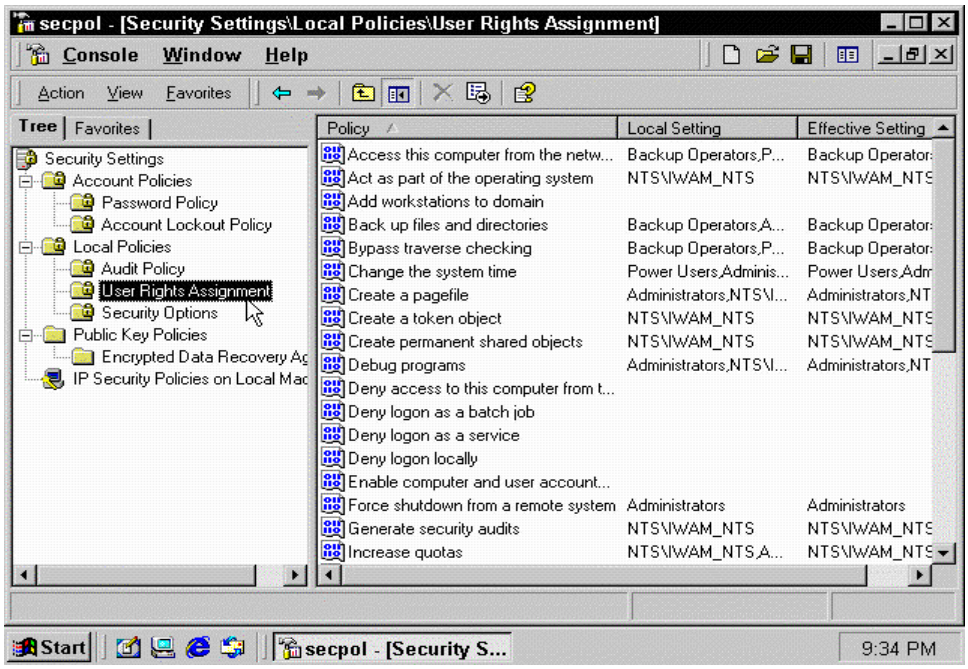
Windows 2000 Professional is the latest edition of the Microsoft Operating System series for end-users. Windows 2000 is based on the Windows NT Kernel and is referred to as Windows NT 5.0. Windows 2000 contains over 29 Million lines of code mainly written in C++. 8 Million of those lines alone are written for drivers. Windows 2000 is one of the largest commercial projects ever attempted. While Windows 2000 Professional is designed to be more secure than Windows NT Workstation 4.0, the truth is an Operating system is only as secure as the safe guards applied by the users, and implemented by workgroup managers and network administrators.

Built on Windows NT technology and the easy-to-use, familiar Windows 98 user interface, Windows 2000 Professional gives users increased flexibility. The integrated Web capabilities let you connect to the Internet from anywhere, at anytime—giving access to host of flexible, cost-effective communication options. In addition, broad peripheral and mobile computer support make Windows 2000 Professional an ideal operating system for a workforce that increasingly relies on notebook computers.

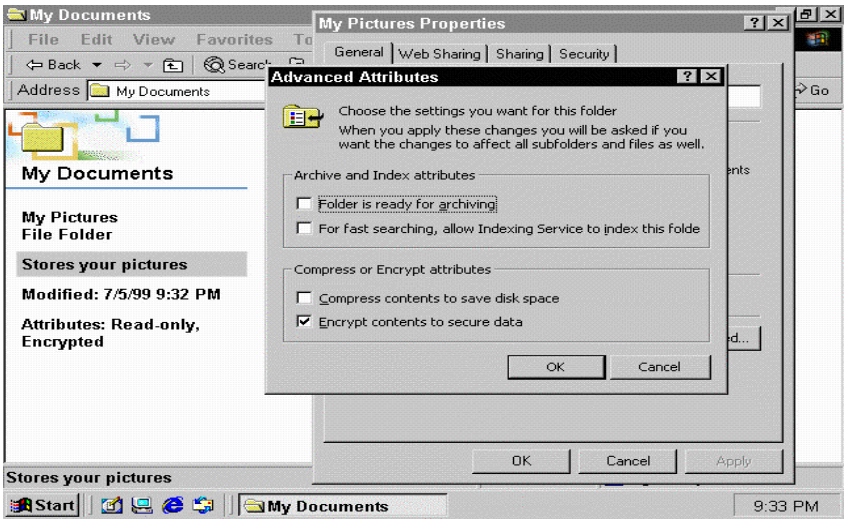
Windows 2000 Professional safeguards:

- Multiple methods of authenticating internal and external users.
- Protection of data stored on disk drives using encryption.
- Protection of data transmitted across the network using encryption.
- Per-property access control for objects.
- Smart card support for securing user credentials.
- Public Key Infrastructure (PKI).

Security: Security in Windows 2000 has been enhanced with the addition of the Security Configuration Manager (SCM), a one-stop security utility that provides access to the entire range of security parameters. Windows 2000 logons now use Kerebos v5 authentication or public key certificates.



Windows 2000 provides an optional Certificate Server for managing deployment of public key certificates. Windows 2000 also implements IPSEC (IP Security Protocol) for encrypted TCP/IP network traffic and the Encrypting File System (EFS) for protecting data on NTFS volumes.



11.6.1 DEFAULT WINDOWS 2000 SECURITY SETTINGS

The default security settings for Windows 2000 can be described by summarizing the permissions granted to four default groups (Administrators, Power Users, Users, and Backup Operators). Members of the Administrators group can perform all functions supported by the operating system. The default security settings allow administrative access to any registry or file system object.

Securing Windows 2000 systems:

- Make sure that end users are members of the Users group only.
- Deploy programs, such as certified Windows 2000 programs, that members of the Users group can run successfully.

Users will not be able to run most programs written for previous versions of Windows because previous versions of Windows either did not support file system and registry security (Windows 95 and Windows 98) or shipped with lax default security settings (Windows NT). If Users have problems running legacy applications on newly installed NTFS systems, then do one of the following:

- Install new versions of the applications that are certified for Windows 2000.
- Move end users from the Users group into the Power Users group.

Decrease the default security permissions for the Users group. This can be accomplished by using the compatible security template. For more information, see "Predefined security templates" in Related Topics.

Administrators can:

Administrators can grant themselves any rights that they do not have by default. Ideally, administrative access should only be used to:

- Install the operating system and components (such as hardware drivers, system services, and so on).
- Install Service Packs and Windows Packs.
- Upgrade the operating system.

- Repair the operating system.
- Configure critical operating system parameters (such as password policy, access control, audit policy, kernel mode driver configuration, and so on).
- Take ownership of files that have become inaccessible.
- Manage the security and auditing logs.

In practice, Administrator accounts often must be used to install and run programs written for previous versions of Windows.

The Users group provides the most secure environment in which to run programs. Group policies are applied in Windows 2000 Active Directory Services. On a volume formatted with NTFS, the default security settings on a newly installed system (but not on an upgraded system) are designed to prevent members of this group from compromising the integrity of the operating system and installed programs. Users cannot modify system-wide registry settings, operating system files, or program files. Users can shut down workstations, but not servers. Users can create local groups, but can manage only the local groups that they created. They can run certified Windows 2000 programs that have been installed or deployed by administrators. Users have full control over all of their own data files (%userprofile%) and their own portion of the registry (HKEY_CURRENT_USER). Individuals cannot install programs that can be run by other Users (this prevents Trojan horse programs). They also cannot access other Users' private data or desktop settings.

Members of the Power Users group have more permissions than members of the Users group and fewer than members of the Administrators group. Power Users can perform any operating system task except tasks reserved for the Administrators group. The default Windows 2000 security settings for Power Users are very similar to the default security settings for Users in Windows NT 4.0. Any program that a User can run in Windows NT 4.0, a Power User can run in Windows 2000.

Power Users can:

- Run legacy applications in addition to Windows 2000 certified applications.
- Install programs that do not modify operating system files or install system services.
- Customize system-wide resources including Printers, Date/Time, Power Options, and other Control Panel resources.
- Create and manage local user accounts and groups.
- Stop and start system services, which are not started by default.

Power Users do not have permission to add themselves to the Administrators group. Power Users do not have access to the data of other users on an NTFS volume, unless those users grant them permission.

Potential Problems and Issues

Running legacy programs on Windows 2000 often requires modify access to certain system settings. The same default permissions that allow Power Users to run legacy programs also make it possible for a Power User to gain additional privileges on the system, even complete administrative control. Therefore, it is important to deploy certified Windows 2000 programs in order to achieve maximal security without sacrificing program functionality. Programs that are certified for Windows 2000 can run successfully under the secure configuration provided by the Users group.

Since Backup Operators can install or modify programs, running as a Power User when connected to, the Internet could make the system vulnerable to Trojan horse programs and other security risks. For more information, see "Why you should not run your computer as an administrator" in Related Topics.

Backup Operators can:

- Back up and restore files on the computer, regardless of any permission that protects those files.
- Log on to the computer and shut it down, but they cannot change security settings.

Potential Problems and Issues

Backing up and restoring data and system files require permissions to read and write those files. The same default permissions granted to Backup Operators that allow them to back up and restore files also make it possible for them to use the group's permissions for other purposes, such as reading another user's files or installing Trojan horse programs. Group Policy settings can be used to create an environment in which Backup Operators only can run a backup program.

Additional Windows 2000 Professional groups

- **Interactive**. This group contains the user who is currently logged on to the computer. During an upgrade to Windows 2000, members of the Interactive group will also be added to the Power Users group, so that legacy applications will continue to function as they did before the upgrade.
- **Network**. This group contains all users who are currently accessing the system over the network.
- **Terminal Server User**. When Terminal Servers are installed in application serving mode, this group contains any users who are currently logged on to the system using Terminal Server. Any program that a user can run in Windows NT 4.0 will run for a Terminal Server User in Windows 2000. The default permissions assigned to the group were chosen to enable a Terminal Server User to run most legacy programs.

Potential Problems and Issues

Running legacy programs in Windows 2000 requires permission to modify certain system settings. The same default permissions that allow a Terminal Server User to run legacy programs also make it possible for a Terminal Server User to gain additional privileges on the system, even complete administrative control. Applications that are certified for Windows 2000 can run successfully under the secure configuration provided by the Users group.

11.6.2 DIFFERENCES BETWEEN WINDOWS NT 4.0 AND WINDOWS 2000 SECURITY SETTINGS

Windows NT 4.0 provided two key groups whose membership could be controlled by the administrator: Administrators and Users. There was one group, everyone, whose membership was controlled by the operating system or domain. Every user who was authenticated by the domain was a member of the everyone group. If an administrator wanted stricter control of access to the computer's resources, the discretionary access control list (DACL) could be modified by removing the everyone group.

Windows 2000 provides three groups whose membership is controlled by the administrator: Users, Power Users, and Administrators. The group whose membership is controlled by the operating system or

domain is Authenticated Users. It is the same as the everyone group, except that it does not contain anonymous users or guests.

Unlike the everyone group in Windows NT 4.0, the Authenticated Users group is not used to assign permissions. Only groups controlled by the administrator, primarily Users, Power Users, and members of the Administrators group, are used to assign permissions. The default members of each group are listed below:

Local Group	Windows 2000 Professional	Windows 2000 Server
Administrators	Administrator	Administrator
Power Users	Authenticated Users	None
Users	Authenticated Users	Authenticated Users

By default in Windows 2000, any authenticated user is a member of the Users group. Windows 2000 Power Users have all the capabilities that Windows NT 4.0 Users had. This ensures backward compatibility with Windows NT 4.0. If an administrator wants to implement higher security on a Windows 2000 computer, Authenticated Users should be made members of the Users group only.

When a Windows 2000 Professional or Server computer joins a domain, the same domain groups are added to the computer that were added to a Windows NT 4.0 computer. Domain Administrators are added to the local Administrators group and Domain Users are added to the local Users group.

11.7 REVIEW QUESTIONS

1. What AFI governs *"Computer Security"*?

2. Workgroup managers contribute to the Air Force mission of information superiority by implementing _____.

3. What elements make up the information security triad?

4. List two elements that ensure data availability.

5. The best Air Force security plan in the world will fail if?

6. To protect the computers in the user's workspace, a network administrator should consider implementing what security measures?

7. Under the concept of *"Access Control,"* provide three means of ensuring unauthorized do not have access to the network.

8. List three elements of strong password policy.

9. What kind of virus or malicious program that is disguised as a harmless program?

10. Why is data protection for remote users difficult?

11. What is the most important think for users to keep in mind when they travel with a laptop computer?